[4] J. A. Buzacott, "Markov approach to finding failure times of repairable systems," *IEEE Trans. Reliability*, vol. R-19, pp. 128–134, 1970.
[5] E. Cinlar, *Introduction to Stochastic Processes*. Englewood Cliffs, NJ: Prentice-Hall, 1975.
[6] R. W. Cottle, "Manifestations of the Schur complement," *Linear Algebra Appl.*, vol. 8, pp. 189–211, 1974.
[7] P. J. Courtois, *Decomposability: Queueing and Computer System Applications*. New York: Academic, 1977.
[8] ——, "On time and space decomposition of complex structures," *Commun. ACM*, vol. 28, pp. 590–603, 1985.
[9] A. Cumani, "Esp—A package for the evaluation of stochastic Petri nets with phase-type distributed transition times," in *Proc. Int. Workshop Timed Petri Nets*, IEEE Computer Society Press no. 674, Torino, Italy, 1985, pp. 144–151.
[10] F. Delebecque, "A reduction process for perturbed Markov chains," *SIAM J. Appl. Math.*, vol. 43, pp. 325–350, 1983.
[11] J. Bechta Dugan, K. S. Trivedi, M. K. Smotherman, and R. M. Geist, "The hybrid automated reliability predictor (HARP)," *AIAA J. Guidance, Contr. Dynam.*, vol. 9, pp. 319–331, 1986.
[12] R. Geist, D. E. Stevenson, and R. A. Allen, "The perceived effect of breakdown and repair on the performance of multiprocessor systems," *Perform. Eval.*, vol. 6, pp. 249–260, 1986.
[13] G. H. Golub and C. F. Van Loan, *Matrix Computation*. Baltimore, MD: John Hopkins University Press, 1983.
[14] A. Goyal, S. Lavenberg, and K. S. Trivedi, "Probabilistic modeling of computer system availability," *Ann. Oper. Res.*, vol. 8, pp. 285–306, 1987.
[15] W. K. Grassmann, "The factorization of queueing equations and their interpretation," *J. Opl. Res. Soc.*, vol. 36, pp. 1041–1050, 1985.
[16] ——, "Transient solution in Markovian queueing systems," *Comput. Oper. Res.*, vol. 4, pp. 47–56, 1977.
[17] D. Gross and D. Miller, "The randomization technique as a modeling tool and solution procedure for transient Markov processes," *Oper. Res.*, vol. 32, pp. 343–361, 1984.
[18] R. A. Howard, *Dynamic Probabilistic Systems, Vol. II: Semi-Markov and Decision Processes*. New York: Wiley, 1971.
[19] L. Kleinrock, *Queueing Systems, Vol. I: Theory*. New York: Wiley-Interscience, 1975.
[20] J. D. Lambert, *Computational Methods in Ordinary Differential Equations*. New York: Wiley, 1973.
[21] J. C. Laprie, "On reliability prediction of repairable redundant digital structures," *IEEE Trans. Reliability*, vol. R-25, pp. 256–258, 1976.
[22] C. D. Meyer and W. J. Stewart, "Computational aspects of stochastic complementation," Tech. Rep., Communication at the ORSA/TIMS Conference on Analysis and Control of Large Scale Stochastic Systems, Chapel Hill, 1988.
[23] J. F. Meyer, "Closed form solution of performability," *IEEE Trans. Comput.*, vol. C-31, pp. 648–657, 1982.
[24] W. L. Miranker, *Numerical Methods for Stiff Equations*. Dordrecht: Reidel, 1981.
[25] A. Reibman and K. S. Trivedi, "Numerical transient analysis of Markov models," *Comput. Oper. Res.*, vol. 15, pp. 19–36, 1988.
[26] ——, "Transient analysis of cumulative measures of Markov chain behavior," *Stochastic Models*, vol. 5, no. 4, pp. 683–710, 1989.
[27] J. R. Rohlicek and A. S. Willsky, "The reduction of perturbed Markov generators: An algorithm exposing the role of transient states," *J. ACM*, vol. 35, pp. 675–696, 1988.
[28] P. J. Schweitzer, "Aggregation methods for large Markov chains," in *Mathematical Computer Performance and Reliability*, P. J. Courtois, G. Iazeolla, and A. Hordijk, Eds. Amsterdam, The Netherlands: North Holland, 1984, pp. 275–285.
[29] C. L. Seitz, "Concurrent VLSI architectures," *IEEE Trans. Comput.*, vol. C-33, pp. 1247–1265, 1984.
[30] D. P. Siewiorek and R. S. Swarz, *The Theory and Practice of Reliable System Design*. Bedford, MA: Digital, 1982.
[31] G. W. Stewart, *Introduction to Matrix Computation*. New York: Academic, 1973.
[32] Y. Takahashi, "Weak D-Markov chain and its application to a queueing network," in *Mathematical Computer Performance and Reliability*, P. J. Courtois, G. Iazeolla, and A. Hordijk, Eds. Amsterdam, The Netherlands: North Holland, 1984, pp. 153–165.
[33] K. Trivedi, *Probability and Statistics with Reliability, Queueing and Computer Science Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1982.
[34] H. Vantilborgh, "Aggregation with an error of $O(\epsilon^2)$," *J. ACM*, vol. 32, pp. 162–190, 1985.

A Characterization of t/s-Diagnosability and Sequential t-Diagnosability in Designs

JOO-KANG LEE AND JON T. BUTLER

***Abstract*—A multiprocessing system is t/s-diagnosable if all faulty processors can be identified to within s processors provided there are no more than t faulty processors. A characterization theorem of Karunanithi and Friedman [4] for t/s-diagnosability in certain special cases of systems called designs is extended to the entire class of $D_{1,t'}(n)$ designs. We show that for large t, s is approximately $t^2/4t'$. Furthermore, the minimum number of processors needed to attain a given diagnosability is derived.**

A multiprocessor system is sequentially t-diagnosable if at least one faulty processor can be identified provided there are no more than t faulty processors. A theorem by Preparata, Metze, and Chien [7] giving a sufficient condition for sequential t-diagnosability in the single loop system, a special case of designs, is extended to the entire class of $D_{1,t'}(n)$ designs. We show that, for large t, approximately $t^2/4t'$ nodes are needed for a $D_{1,t'}(n)$ design to be sequentially t-diagnosable.

***Index Terms*—Multiprocessing systems, reliable computing, systems diagnosis, t-diagnosable, t/s-diagnosable, testing.**

I. Introduction

In the systems diagnosis approach to reliable computing, fault location is achieved by tests among processors. We assume that fault-free processors produce test results that are a true representation of the tested processor, fail if it is faulty and pass if it is fault-free. In the case of faulty processors, however, the test results by such processors may not be correct. The goal is to determine exactly which processors are faulty. However, if there are too many faulty processors, incorrect test information can cause ambiguity.

Our model is that of Preparata, Metze, and Chien [7]. A *system* S is a directed graph where nodes represent processors and arcs represent tests among processors. Node u_i tests node u_j iff there is a directed arc from u_i to u_j. Each node has one of two states, *faulty* or *fault-free*, and each arc has one of two weights, *pass* or *fail*. For example, Fig. 1 shows a system of 12 nodes and two arrangements of three faulty nodes, which are indicated by X's. Fail test outcomes are indicated by 1's, while unmarked arcs correspond to pass outcomes.

A system is (*one-step*) *t-diagnosable* if all faulty nodes can be uniquely identified provided there are no more than t of them. For example, the system in Fig. 1 is *not* 3-diagnosable because the set of test outcomes shown in Fig. 1(b), which is produced with u_3, u_4, and u_5 faulty, can also be produced with just u_3 and u_4 faulty. Thus, if we assume there are three or fewer faulty nodes in the system, u_5 cannot be uniquely identified as faulty. t-diagnosability represents worst case conditions. For example, the three faulty nodes in Fig. 1(a) are uniquely faulty.

S is a $D_{\delta,t'}(n)$ *design* iff an arc exists from node u_i to u_j for

Manuscript received October 23, 1987; revised September 4, 1988 and January 4, 1989. J. T. Butler was supported by a NAVELEX Chair Professorship tenured at the Naval Postgraduate School and by NSF Grant ECS-8203276.

J.-K. Lang is with the POSTECH Research Institute of Science and Technology, Pohang City, Kyungbuk 680, Korea.

J. T. Butler is with the Department of Electrical and Computer Engineering, Naval Postgraduate School, Monterey, CA 93943.

IEEE Log Number 9035141.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 1989		

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Characterization of t/s-Diagnosability and Sequential t-Diagnosability in Designs	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Naval Postgraduate School,Department of Electrical and Computer Engineering,Monterey,CA,93943	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

multiprocessing system is t/s-diagnosable if all faulty processors can be identified to within s processors provided there are no more than t faulty processors. A characterization theorem of Karunanithi and Medman 14) for 0s-diagnosability in certain special cases of systems called designs is extended to the entire class ofDl,,,(n) designs. We show that for large t , s is approximately t2/4t?. Furthermore the minimum number of processors needed to attain a given diagnosability is derived. A multiprocessor system is sequentially t-diagnosable if at least one faulty processor can be identified provided there are no more than t faulty processors. A theorem by Preparata, Metze, and Chien 171 giving a sufficient condition for sequential t -diagnosability in the single loop system, a special case of designs, is extended to the entire class of D I , ~ . (de~si)g ns. We show that, for large t , approximately t2/4t ? nodes are needed for a Dl,,.(n) design to be sequentially t-diagnosable.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**7**	

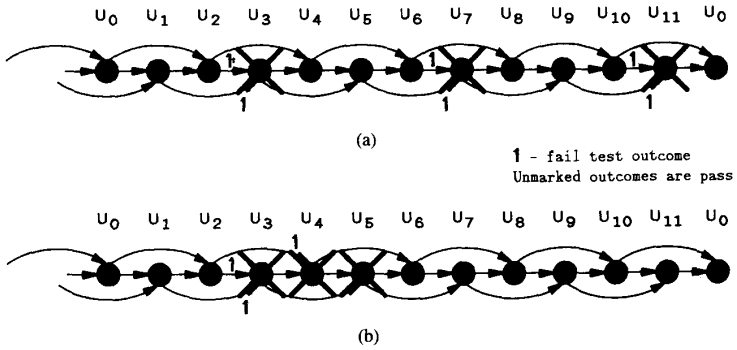


Fig. 1. Examples of a $D_{1,2}(12)$ design.

$j - i = \delta p \bmod n$, and p assumes the values $1, 2, \cdots, t'$, where n is the number of nodes [7]. For example, the system in Fig. 1 is a $D_{1,2}(12)$ design. From [7], $D_{\delta,t'}(n)$ is t'-diagnosable iff $n \geq 2t'+1$. Thus, the system of Fig. 1 is 2-diagnosable. Preparata, Metze, and Chien [7] observe that, when δ and n are relatively prime, a $D_{\delta,t'}(n)$ design is isomorphic to a $D_{1,t'}(n)$ design. Thus, the diagnosability of the former is identical to that of the latter. In the following, we restrict our attention to $D_{1,t'}(n)$ designs, with the recognition that a larger class of systems is characterized.

When the number of faulty nodes exceeds t in a t-diagnosable system, it may be necessary to replace fault-free nodes in order to replace all faulty nodes. A system is *t/s-diagnosable* iff all faulty nodes can be identified to within a set of s nodes, provided there are no more than t faulty nodes. s depends on t. For example, from previously published results [4] and from results in this paper, we can conclude that $D_{1,2}(12)$ is t/s-diagnosable for $t/s = 1/1$, 2/2, 3/4, 4/6, 5/8, and i/12, where $6 \leq i \leq 12$. The last result, i/12, also follows from an observation in [7], that when the number of faulty nodes equals or exceeds the number of fault-free nodes, the ambiguity of the fault/fault-free status of nodes can extend to the entire set of nodes.

Building on results of Freidman [2], Karunanithi and Friedman [4] characterize t/s-diagnosability in two special cases of $D_{1,t'}(n)$ designs,

$$1) \quad t' = 1, \quad \text{and} \tag{1}$$

$$2) \quad t' > \left\lfloor \frac{t}{2} \right\rfloor. \tag{2}$$

That is, for these two cases, an expression is derived for s as a function of t when a minimal number $n_{\min}$ of nodes exists. Furthermore, an expression for $n_{\min}$ is derived. We extend this result to $2 \leq t' \leq \lfloor t/2 \rfloor$, covering all other cases of $D_{1,t'}(n)$ designs. We show that, for such designs, both s and $n_{\min}$ are approximately $t^2/4t'$ when t is large. Thus, the status of almost all nodes in designs with a near minimal number of nodes can be uncertain in the worst case.

A system is *sequentially t-diagnosable* iff at least one faulty node can be identified provided there are no more than t of them. Preparata, Metze, and Chien [7] show a lower bound ν on the number of nodes n in a special case of $D_{1,1}(n)$ designs, called single loop systems, such that such systems are sequentially t-diagnosable. That is, it is shown that if $n \geq \nu$, then $D_{1,1}(n)$ is sequentially t-diagnosable, where ν depends on t'. We extend this result to all $D_{1,t'}(n)$ designs. For example, $D_{1,2}(12)$ in Fig. 1 is sequentially 5-diagnosable. Specifically, we show a lower bound $n_{\min}$ on the number of nodes n such that, if $n \geq n_{\min}$, a $D_{1,t'}(n)$ design is sequentially t-diagnosable. For example, $D_{1,2}(n)$ is sequentially 5- and 6-diagnosable for $n \geq 11$ and $n \geq 13$, respectively.

Neither t/s-diagnosability nor sequential t-diagnosability have been characterized in general systems. Chwa and Hakimi [1] characterize t/t-diagnosability, a topic originally studied by Kavianpour and Friedman [5]. Yang, Masson, and Leonetti [10] give a polynomial time algorithm, in which all faulty nodes in a t/t-diagnosable system can be identified except perhaps at most one node, whose status is in doubt. Manber [6] extends the class of known sequentially t-diagnosable systems to certain strongly connected systems. Somani, Agrawal, and Davis [8] characterize the diagnosability of *fault sets* in systems. Sullivan [9] was the first to give necessary and sufficient conditions for t-diagnosability in general systems which can be checked in polynomial time, unlike previous exponential time conditions [3].

II. Background

We can divide nodes into three categories.

Definition: Given a system, a set of test outcomes σ, and an integer f, a node u is *definitely good* (*definitely bad*) with respect to σ if the assumption that u is faulty (fault-free) implies there are more than f faulty nodes. A node which is neither definitely good nor definitely bad is *suspect*.

For example, for $f = 3$ and for the set of test outcomes shown in Fig. 1(b), u_2, u_3, and u_5 is a definitely good, definitely bad, and suspect node, respectively. Note that for any set of test outcomes produced by any arrangement of t or fewer faulty nodes in a t-diagnosable system, the definitely bad nodes correspond exactly to the faulty nodes, when $f = t$. Furthermore, there are no suspects. The t-diagnosability of the system precludes such ambiguity. There can be as many as s suspects in a t/s-diagnosable system. For example, in the $D_{1,2}(12)$ system of Fig. 1, which is i/12-diagnosable for $6 \leq i \leq 12$, when there are six or more faulty nodes, each of the 12 nodes in the system is suspect if all faulty nodes fail fault-free nodes they test and pass faulty nodes they test. From the results shown below, if at least one faulty node can be identified in a $D_{1,t'}(n)$ design, there can be as many as $s - t'$ suspects.

Let F denote a set of faulty nodes in a system S, where $|F| \leq t$. Let σ be a *syndrome* or set of test outcomes produced by F. FR is a *replacement set generated by F through* σ if

$$FR = \bigcup_i F_i \tag{3}$$

where F_i produces σ and $|F_i| \leq t$. It follows that $u \in FR$ iff u is definitely bad or suspect with respect to σ. The term *replacement set* is used to indicate that, in order to replace all faulty nodes, all nodes in the replacement set must be replaced by fault-free nodes. Each definitely bad node is common to all F_i, while each suspect is missing from at least one F_i. FR is a *maximal replacement set* if there is no larger replacement set with respect to *any* set of test outcomes σ produced by *any* fault set of t or fewer nodes. In a t/s-diagnosable system, $s = |FR|$, where FR is a maximal replacement set.

III. Results

The diagnosability of a system reflects *worst case* conditions. That is, in a t/s-diagnosable system, all faulty nodes can *always* be identified to within a set of size s provided that there are no more than

t faulty nodes. However, for a specific arrangement of faulty nodes, it may be possible to identify the faulty nodes to within a set of size *smaller* than s.

Our main result, Theorem 1, gives necessary and sufficient conditions for a $D_{1,t'}(n)$ design to be t/s-diagnosable. We proceed by showing worst case conditions, the largest replacement set among all replacement sets associated with fault sets of t or fewer nodes. Lemma 1 shows that such a set consists of consecutive nodes. Lemmas 2 and 3 give characteristics of a certain fault set which produces the largest replacement set. Theorem 1 establishes the size of the largest replacement set.

Lemma 1: Let FR be a maximal replacement set in a $D_{1,t'}(n)$ design corresponding to a set of test outcomes produced by a fault set of size t or smaller, where $t > t'$. Then, FR is a set of consecutive nodes.

Proof: On the contrary, assume there exists a maximal replacement set FR consisting of $p \geq 2$ segments, $B_0, B_1, \cdots, B_{p-1}$, of definitely bad and suspect nodes separated by definitely good nodes, where the direction of tests is toward increasing index. Because of the intervening definitely good nodes, if $|B_j| \leq t'$, all nodes in B_j are definitely bad, and if $|B_j| > t'$, the first t' nodes are definitely bad, while the remaining are suspect. Furthermore, since $t > t'$, there is at least one suspect in a maximal replacement set, FR. On the contrary, if all nodes in FR are definitely bad, $|FR| \leq t$, since there can be no more definitely bad nodes than faulty nodes. However, $|FR| > t$, as illustrated by the following; consider syndrome σ produced by a sequence of t consecutive faulty nodes $F = \{u_k, u_{k+1}, \cdots, u_{k+t-1}\}$, where all test results by faulty nodes are pass except for the test of fault-free node u_{k+t} by faulty node u_{k+t-1}, which is fail. Node u_{k+t} is tested by faulty nodes exclusively, and, since $t > t'$, its faulty/fault-free status cannot be uniquely determined. The replacement set in this case contains at least $t + 1$ elements. So also does a maximal replacement set, FR. Since there is at least one suspect, there is at least one segment B_i containing a suspect, and $|B_i| > t$.

Let G_i be the definitely good nodes between B_i and B_{i+1}, where index addition is mod p. Since the direction of tests is toward increasing index, nodes in B_i test nodes in G_i, and nodes in G_i test nodes in B_{i+1}. Given a sequence of nodes B, ${}^*B$ is B if $|B| \leq t'$ and is the first t' nodes of B beginning with the (unique) node in B not tested by another node in B, if $|B| > t'$. We now show that a sequence of $|{}^*B_{i+1}|$ nodes in G_i nearest B_i can be converted to suspect nodes.

Indeed $|G_i| > |{}^*B_{i+1}|$, as follows. Nodes that are definitely bad in FR correspond to nodes that are faulty in all fault sets which generate FR. Thus, if F is a fault set which generates FR through σ, then tests by such nodes are arbitrary. Consider the case where tests by definitely bad nodes are all pass. All nodes in G_i are tested by definitely bad and suspect nodes in B_i. Furthermore, all suspects in B_i which test nodes in G_i must produce pass test outcomes; no suspect fails a definitely good node. Then, regardless of other test outcomes, $F' = F \cup G_i -^* B_{i+1}$ is a fault set which generates FR through σ. If $|G_i| \leq |{}^*B_{i+1}|$, $|F'| \leq |F| \leq t$, and nodes in G_i are suspect, not definitely good, as assumed. Then, it must be that $|G_i| > |{}^*B_{i+1}|$.

Let G_1^{**} be the $|{}^*B_{i+1}|$ nodes in G_i just preceding B_{i+1}. Form a new system by removing the sequence of nodes $G_i - G_1^{**}$ along with tests by these nodes and inserting them immediately before the definitely bad nodes in B_i. The severed tests are applied in their original order, so that the resulting system is a $D_{1,t'}(n)$ design. Retain the outcomes of all tests, except

1) Test outcomes of tests applied by nodes in $G_i - G_i^{**}$ after rearrangement agree with the definitely good node immediately preceding B_i before rearrangement,

2) Test outcomes of tests applied by nodes in G_{i-1} to nodes in B_i after rearrangement agree with the test outcomes before rearrangement of the definitely good node immediately preceding B_i. Test outcomes of the tests applied by nodes in G_{i-1} to nodes $G_i - G_i^{**}$ after rearrangement are all pass, and

3) Test outcomes of tests applied by nodes in B_i to nodes in G_i^{**} and follow on nodes agree with the test results of the node in $G_i - G_i^{**}$ immediately preceding G_i^{**} before rearrangement.

By virtue of the choice of test outcomes, a fault set F consistent with the syndrome before rearrangement is consistent after. However, $F' = F \cup G_i^{**} -^* B_{i+1}$ is now also consistent. Since $|F'| = |F| \leq t$, nodes in G_i^{**} are now suspect, as are nodes in ${}^*B_{i+1}$. Thus, the total number of definitely bad nodes and suspects is larger. It follows that FR is not a maximal replacement set as assumed. Q.E.D.

For the interested reader, the Appendix illustrates the proof of Lemma 1 using a specific design. In a t/s-diagnosable system, if there are t or fewer faulty nodes, their location extends, in the worst case, to a set of s nodes. From Lemma 1, this worst case corresponds to consecutive nodes. The next two lemmas concern the characteristics of fault sets for this worst case situation.

Lemma 2: Let FR be a maximal replacement set in a $D_{1,t'}(n)$ design with $t > t'$ faulty nodes. If there is at least one definitely good node, then there exists a fault set F which generates FR such that each faulty node in F belongs to a sequence of consecutive faulty nodes of length t' or more.

Proof: Assume there is at least one definitely good node, and let FR be a maximal replacement set in $D_{1,t'}(n)$. Let σ be a set of test outcomes and F' be a set of t or fewer nodes such that F' generates FR through σ. F' consists of segments $F_0, F_1, \cdots, F_{q-1}$ of consecutive faulty nodes separated by fault-free nodes, where the direction of tests is toward increasing index. We proceed by showing that, if there is at least one segment F_i such that $|F_i| < t'$, then there is another fault set F which generates FR, where all nodes in F belong to a sequence of consecutive faulty nodes each of length t' or more.

It is sufficient to show that under the above conditions, we can join F_i with F_{i-1} without changing FR, where index subtraction is mod q. Indeed, there is at least one other segment, since $|F_i| < t'$ and $t > t'$. Let FF_i be the segment of fault-free nodes immediately following F_i, where the direction of tests is from F_i towards FF_i.

Since there is at least one definitely good node, there is a definitely good node u immediately preceding FR. From Lemma 1, FR is a set of consecutive nodes, and it has length greater than t'. Thus, all outcomes of tests by u are fail. On the contrary, if any test outcome is pass, the tested node must be definitely good. Thus, the first t' nodes of FR are definitely bad, while all subsequent nodes in FR are suspect. Since $|F_i| < t'$, F_i does not contain the first t' definitely bad nodes, and so F_i contains only suspect nodes, while F_{i-1} consists of suspects and/or definitely bad nodes. Similarly, FF_i consists of suspects and/or definitely good nodes. Let $FF_{i-1/i} = FF_{i-1} \cup \{\text{suspects in } FF_i\} = \{u_0, u_1, \cdots, u_g\}$. Furthermore, assume that the indexes correspond to the natural order of nodes as determined by tests. That is, $u_0, u_1, \cdots$, and $u_{|FF_{i-1}|-1}$ correspond to the nodes of FF_{i-1}, such that u_0 tests u_1, u_1 tests u_2, etc. Similarly, $u_{|FF_{i-1}|}$ is the first suspect in FF_i, $u_{|FF_{i-1}|+1}$ is the second, etc. Because nodes in FF_{i-1} and FF_i are fault-free, all tests among nodes in $FF_{i-1/i}$ are pass. Since u_g is suspect, there is a fault set F'', where $|F''| \leq t$ which generates FR through σ, such that $u_g \in F''$. Since there is a path of pass test outcomes from any $u_j \in FF_{i-1/i}$ to u_g, $u_j \in F''$. Thus, $u_g \in F''$ implies $FF_{i-1/i} \subseteq F''$.

Besides F' and F'', there are other sets which generate FR through σ. F'', which contains the first k nodes of $FF_{i-1/i}$, where $1 < k < |FF_{i-1/i}|$, is consistent with σ. However, $F'' \cup F''' = F''$, and since $|F''| \leq t$, then $|F'''| \leq t$. Therefore, it is sufficient to consider fault sets which contain all members of $FF_{i-1/i}$ or no members of $FF_{i-1/i}$.

Note that this observation is independent of the position of F_i within $FF_{i-1/i}$. Specifically, the following rearrangement of nodes and tests leaves FR unchanged, but produces a fault set generating FR which is the same as F' except F_{i-1} and F_i are combined as a single sequence of faulty nodes. That is, all nodes in F_i plus all tests by F_i are inserted between F_{i-1} and FF_{i-1}. All tests are reconnected in their natural order, and all test results among faulty nodes after rearrangement are pass. Q.E.D.

From Lemma 1, a maximal replacement set FR in a $D_{1,t'}(n)$ design corresponding to a set of $t > t'$ faulty nodes consists of con-

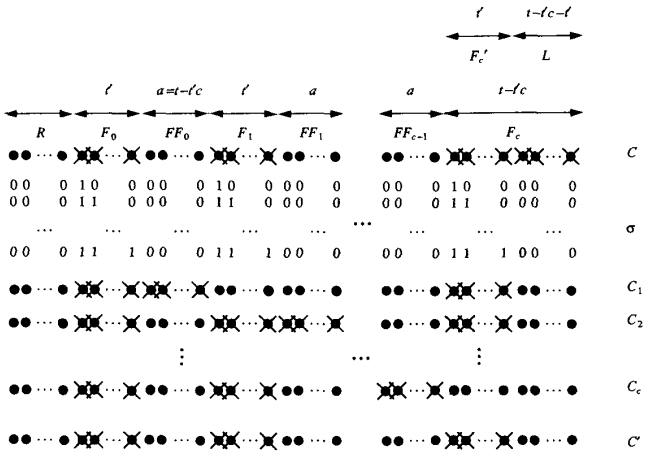


Fig. 2. The canonic fault set.

secutive nodes. From Lemma 2, there is a fault set F which generates FR where all nodes in F belong to segments of consecutive nodes of length at least t'. Also, from the proof, it is clear that F generates FR through a set of test outcomes σ where no faulty node fails another faulty node. Thus, fail test outcomes in σ occur only between nodes of different status, and σ consists of c groups of fail test outcomes separated by pass test outcomes. Let C be a *canonic* fault set which generates a maximal replacement set FR iff all nodes in C belong to segments of consecutive nodes of length t' or greater with at most one segment having length strictly greater than t'. The existence of C is assured because it is consistent with σ. That is, each of the c groups of fail test outcomes in σ corresponds to t' faulty nodes with the last group (farthest from the definitely bad nodes in FR in the direction of tests) having an additional $t - t'c$ consecutive faulty nodes.

Lemma 3: Let FR be a maximal replacement set in a $D_{1,t'}(n)$ design with $t > t'$ faulty nodes. If there exists at least one definitely good node, a segment of suspect fault-free nodes FF_i that follows a segment of faulty nodes in a canonic fault set which generates FR has the property

$$|FF_i| = t - t'c \tag{4}$$

where $c \in \{\lceil t/2t' \rceil, \lfloor t/2t' \rfloor\}$ such that $c(t - t'c) + t$ has maximum value.

Proof: Let $F_0, F_1, \cdots$, and F_k be the segments of consecutive faulty nodes in C, and let FF_i be the fault-free nodes between F_i and F_{i+1}. Because $t > t'$, $k \geq 1$. If there is at least one definitely good node, one segment is definitely bad. Let F_0 be the set of t' definitely bad nodes in FR, and let σ be the syndrome which generates FR in which all faulty nodes produce pass test outcomes. Since F_{i+1}, for $0 \leq i \leq k-1$, is a set of suspects, there is another fault set not containing F_{i+1}. But this implies containment of FF_i. Since $|F_j| = t'$ (by Lemma 2 and the definition of C), there are no tests between adjacent FF_j's. Thus, a smallest fault set F such that $F_{i+1} \not\subseteq F$ is $F = C - L - F_{i+1} \cup FF_i$, where L is the last $t - t'c - t'$ faulty nodes in F_k in the direction of tests. The fail test outcomes at the site of each of the k other F_i imply at least t' faulty nodes. Since $|C - L| = t'(k+1)$ and $|FF_{i+1}| = t'$, it follows that $|FF_i| + t'k \leq t$. Thus, $|FF_i| \leq t - t'k$. But FR is a maximal replacement set, and so

$$|FF_i|_{\max} = t - t'k, \tag{5}$$

and

$$s = k|FF_i|_{\max} + t. \tag{6}$$

From (5) and (6), we have

$$s = k(t - t'k) + t \tag{7}$$

where k is chosen so that ds/dk is 0. Thus, $k = \lceil t/2t' \rceil$ or $\lfloor t/2t' \rfloor$. Q.E.D.

Lemma 2 and the observations that follow it show that the canonic fault set C generates a maximal replacement set FR. Lemma 3 shows that the number of fault-free nodes separating segments of faulty nodes in C has some maximum value, $t - t'c$. Fig. 2 shows the canonic fault set C and a syndrome σ produced by it. Each column associated with σ corresponds to the test results of the node just above the column. 0 is pass and 1 is fail. That is, in a $D_{1,t'}(n)$ design, node u_i tests u_j iff $j - i = p \bmod n$, where $p = 1, 2, \cdots, t'$. The top row of test results corresponds to $p = 1$, the second corresponds to $p = 2, \cdots$, and the last corresponds to $p = t'$. Thus, the leftmost node in F_i fails all tests applied to it, since these are by fault-free nodes. The next node fails all but one test, that by the faulty node just to its left, etc. Fig. 2 also shows other fault sets $C_1, C_2, \cdots$, and C_c which generate σ. Note that in C_i the nodes just preceding F_i in C are faulty. These are nodes which are fault-free with respect to F, and thus are suspect nodes, since $|C_i| = t$. Since these nodes are fault-free in C, they are suspect nodes. Fig. 2 also shows C', the fault set with fewest nodes $(c+1)t'$ which generates FR.

Since nodes in R are definitely good, the assumption that any one is faulty leads to the conclusion that there are more than t faulty nodes in the system. This imposes a lower bound on the size of R. For example, if the node in R immediately preceding F_0 is faulty, then so also are all nodes in R, as well as all nodes in the segment of $t - t'c - t'$ nodes labeled L in Fig. 2. The smallest number of remaining faulty nodes that is consistent with the fail test outcomes is ct', all nodes in C' less those in F_0. Thus, we require $|R| + t - t'c - t' + t'c = |R| + t - t' > t$ or

$$|R| > t'. \tag{8}$$

This observation is a part of the proof of Theorem 1.

Theorem 1: Design $D_{1,t'}(n)$ is t/s-diagnosable iff

$$n \geq n_{\min} = s + \min(t, t') + 1 \tag{9}$$

where

$$s = \max\left(\left\lceil \frac{t}{2t'} \right\rceil \left(t - t' \left\lceil \frac{t}{2t'} \right\rceil\right), \left\lfloor \frac{t}{2t'} \right\rfloor \left(t - t' \left\lfloor \frac{t}{2t'} \right\rfloor\right)\right) + t. \tag{10}$$

TABLE I
s AND $n_{\min}$ FOR t/s-DIAGNOSABILITY AND SEQUENTIAL t-DIAGNOSABILITY IN $D_{1,t'}(n)$ DESIGNS, WHERE $n \geq n_{\min}$. ENTRIES REPRESENT $s/n_{\min}$

t/t'	1	2	3	4	5	6	7	8	9	10
1	1/3	1/3	1/3	1/3	1/3	1/3	1/3	1/3	1/3	1/3
2	3/5	2/5	2/5	2/5	2/5	2/5	2/5	2/5	2/5	2/5
3	5/7	4/7	3/7	3/7	3/7	3/7	3/7	3/7	3/7	3/7
4	8/10	**6/9**	5/9	4/9	4/9	4/9	4/9	4/9	4/9	4/9
5	11/13	**8/11**	7/11	6/11	5/11	5/11	5/11	5/11	5/11	5/11
6	15/17	**10/13**	**9/13**	8/13	7/13	6/13	6/13	6/13	6/13	6/13
7	19/21	**13/16**	**11/15**	10/15	9/15	8/15	7/15	7/15	7/15	7/15
8	24/26	**16/19**	**13/17**	**12/17**	11/17	10/17	9/17	8/17	8/17	8/17
9	29/31	**19/22**	**15/19**	**14/19**	13/19	12/19	11/19	10/19	9/19	9/19
10	35/37	**22/25**	**18/22**	**16/21**	**15/21**	14/21	13/21	12/21	11/21	10/21
11	41/43	**26/29**	**21/25**	**18/23**	**17/23**	16/23	15/23	14/23	13/23	12/23
12	48/50	**30/33**	**24/28**	**20/25**	**19/25**	**18/25**	17/25	16/25	15/25	14/25
13	55/57	**34/37**	**27/31**	**23/28**	**21/27**	**20/27**	19/27	18/27	17/27	16/27
14	63/65	**38/41**	**30/34**	**26/31**	**23/29**	**22/29**	**21/29**	20/29	19/29	18/29
15	71/73	**43/46**	**33/37**	**29/34**	**25/31**	**24/31**	**23/31**	22/31	21/31	20/31
16	80/82	**48/51**	**37/41**	**32/37**	**28/34**	**26/33**	**25/33**	**24/33**	23/33	22/23
17	89/91	**53/56**	**41/45**	**35/40**	**31/37**	**28/35**	**27/35**	**26/35**	25/35	24/35
18	99/101	**58/61**	**45/49**	**38/43**	**34/40**	**30/37**	**29/37**	**28/37**	**27/37**	26/37
19	109/111	**64/67**	**49/53**	**41/46**	**37/43**	**33/40**	**31/39**	**30/39**	**29/39**	28/39
20	120/122	**70/73**	**53/57**	**44/49**	**40/46**	**36/43**	**33/41**	**32/41**	**31/41**	**30/41**

Proof: There are two cases, $t \leq t'$ and $t > t'$. For $t \leq t'$, $s = t$ and the inequality becomes $n \geq n_{\min} = 2t + 1$, which is necessary and sufficient for t/s-diagnosability in $D_{1,t'}(n)$ designs, where $\lfloor t/2 \rfloor \leq t'$, as given in Theorem 3 of [4]. (The expansion for s in Theorem 3 of [4], $s = 2t - t'$, is valid only for $t \geq t'$. For $t < t'$, the correct expression is $s = t$.)

Now consider the second case.

(if) Assume the condition holds, but S is not t/s-diagnosable. Then, there exists a fault set F where $|F| \leq t$ which generates a replacement set FR such that $|FR| > s$, where s is given in (10). However, it follows from Lemma 3 that, if there is at least one definitely good node, a maximal replacement set FR' consists of c segments of nodes that are fault-free in the canonic fault set, each having size $t - t'c$, plus the t faulty nodes in C, for a total of $c(t - t'c) + t$ nodes, where c is either $\lceil t/2t' \rceil$ or $\lfloor t/2t' \rfloor$ depending on which produces the maximum value of $c(t - t'c) + t$. Thus, it must be that there is no definitely good node, and all nodes are suspect. Specifically, nodes in $R = V - FR'$, where V is the set of all nodes, are suspect. We now show that this leads to a contradiction, and it must be that S is indeed t/s-diagnosable.

It follows that $|R| = n - s$. Since $t > t'$, $\min(t, t') = t'$, and from (9), $n - s \geq t' + 1$. Thus, $|R| \geq t' + 1$. Since nodes in R are suspect, the set $F' = C \cup R - F_0$ is a set of smallest size where nodes in R are faulty which is consistent with a set of test outcomes produced by C and where F_0 is the set of nodes that would be definitely bad if at least one definitely good node exists. Since $C \cap R = \phi$ and $F_0 \subseteq C$, we have

$$|F'| = |R| + t - |F_0| \geq t' + 1 + t - t' = t + 1 \qquad (11)$$

which is a contradiction.

(only if) Suppose that S is t/s-diagnosable, but $n < s + t' + 1$. Since $n < s + t' + 1$, the set R of definitely good nodes is no larger than t' in the worst case of a replacement set of s nodes, where s is given in the hypothesis. However, the set of test outcomes produced by a canonic fault set C can also be produced by $F' = C \cup R - F_0$. Since $|F'| = |F| = t$, R consists of suspects, not definitely good nodes. Q.E.D.

For the special case of $t' = 1$, Theorem 1 applies to the single loop system. The statement in this case is identical to that of Theorem 1 of [4]. It follows from Theorem 1 that in a $D_{1,t'}(n)$ design if $n < n_{\min}$, then there exists a set of t faulty nodes and a set of test outcomes such that this system is not sequentially t-diagnosable. Conversely, from Theorem 1, if $n \geq n_{\min}$, there is no arrangement of t faulty nodes and no set of test outcomes such that all nodes are suspect. Since at least one faulty node can be identified, such a system is sequentially t-diagnosable. Thus, we have the following.

Corollary: Design $D_{1,t'}(n)$ is sequentially t-diagnosable iff

$$n \geq n_{\min} = s + \min(t,' t') + 1 \qquad (12)$$

where

$$s = \max\left\{\left(\left\lceil \frac{t}{2t'} \right\rceil \left(t - t' \left\lfloor \frac{t}{2t'} \right\rfloor\right), \left\lfloor \frac{t}{2t'} \right\rfloor \left(t - t' \left\lfloor \frac{t}{2t'} \right\rfloor\right)\right) + t. \qquad (13)$$

IV. CONCLUDING REMARKS

Table I shows the value of s and $n_{\min}$ such that a $D_{1,t'(n)}$ design is t/s-diagnosable for $n \geq n_{\min}$. t' varies across the columns and t varies down the rows. Each entry is $s/s_{\min}$. The column headed by $t' = 1$ corresponds to a single loop system and $n_{\min}$ in this column agrees, as it should, with the values derived by Preparata, Metze, and Chien [7] for the lower bound on n such that a single loop system is sequentially t-diagnosable. The nonbold data represent previous results. For example, the nonbold data associated with $t' > \lfloor t/2 \rfloor$ is that of Karunanithi and Friedman [4], while the nonbold data associated with $t' = 1$ is from [4] and [7]. The bold data represent data from the results of this paper not covered by these previous papers.

Fig. 3 shows a three-dimensional plot of s versus t with t' as a parameter for $1 \leq t' \leq 10$. The thin lines represent the data derived from the results of Karunanithi and Friedman [4], while the heavy lines represent the data derived by the results of this paper. This shows that, compared to higher order designs, it is much more difficult to locate faults in single loop systems. That is, as one progresses towards designs with more tests, a smaller maximal replacement set

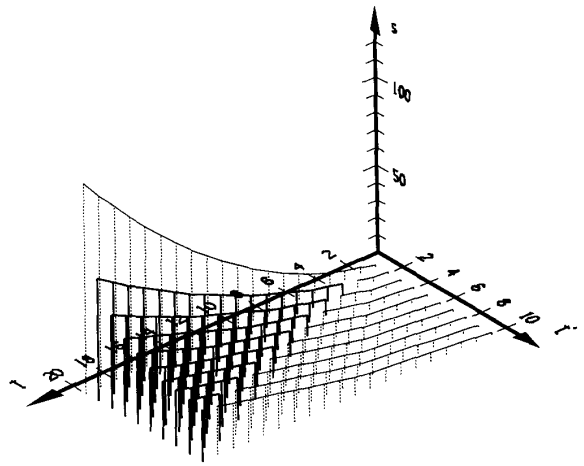


Fig. 3. s versus t and t' required for t/s-diagnosability in $D_{1,t'}(n)$ designs, for $1 \le t' \le 10$ and $1 \le t \le 20$.

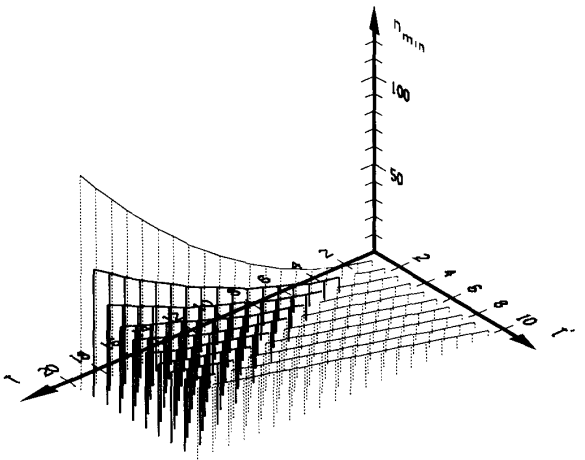


Fig. 4. $n_{\min}$ versus t and t' required for t/s-diagnosability in $D_{1,t'}(n)$ designs, for $1 \le t' \le 10$ and $1 \le t \le 20$, where $n \ge n_{\min}$.

is required for some fixed number of faults in the design. However, a point of diminishing returns is reached, where added tests produce only marginally smaller maximal replacement sets.

We can obtain a simple expression for s as a function of t and t' for large t. Let $g(t) \sim h(t)$ mean $\lim_{t\to\infty} g(t)/h(t) = 1$. Then, the expressions within the ceiling and floor brackets of (10) can be replaced as follows: $\lfloor t/2t' \rfloor \sim t/2t'$ and $\lceil t/2t' \rceil \sim t/2t'$, in which case, the arguments of the max operator in (10) have the same form, and we can write

$$s \sim \frac{t^2}{4t'}. \tag{14}$$

For large t, s is directly proportional to t^2 and inversely proportional to t'. Thus, the curves for fixed t' in Fig. 3 are approximately half parabolas. This is most evident in the curve for $t' = 1$. It is also worth noting that for small t, specifically, $t \le t'$, s is the linear function $s = t$, since, for this case, all faulty nodes can be uniquely identified. This is most evident in the curve for $t' = 10$.

Fig. 4 shows a three-dimensional plot of $n_{\min}$ versus t' and t. This resembles the plot of Fig. 3 and shows the large influence of the s term in the expression for $n_{\min}$. The thin lines represent data due to Karunanithi and Friedman [4] and Preparata, Metze, and Chien [7], while the heavy lines represent data derived from results of this paper. Similarly, it can be seen that

$$n_{\min} \sim \frac{t^2}{4t'}. \tag{15}$$

Thus, for large t, approximately $t^2/4t'$ nodes are necessary for a $D_{1,t'}(n)$ design to be sequentially t-diagnosable.

It is interesting that as little as $t' + 1$ definitely good nodes can exist in a t/s-diagnosable system (the minimum number of nodes in R, as shown in Theorem 1) and that as little as t' definitely bad nodes can exist. So, while the number of suspects grows quadratically, the minimum number of definitely good and definitely bad nodes remains constant. Thus, as t increases, the fraction of the total number of nodes that are suspect can approach 100%.

Appendix

Example Illustrating the Proof of Lemma 1

Lemma 1: Let FR be a maximal replacement set in a $D_{1,t'}(n)$ design corresponding to a set of test outcomes produced by a fault set of size t or smaller, where $t > t'$. Then, FR is a set of consecutive nodes.

Proof: Proceeds by contradiction. That is, we assume there exists a maximal replacement set FR which does *not* consist of consecutive nodes and show that this is impossible. Specifically, we show that we can rearrange certain nodes (without changing their fault-free/faulty status) to produce a replacement set that is larger than FR.

As an example of the proof, consider the $D_{1,2}(19)$ design shown in Fig. 5. The syndrome shown consists of six fail test outcomes (indicated by 1). If $t = 8$, there can be at most eight faulty nodes. With $t = 8$, there are four definitely bad nodes divided into two subsets $\{u_4, u_5\}$ and $\{u_{13}, u_{14}\}$ (indicated by shading consisting of vertical lines). These are definitely bad because, if any one is fault-free, there are more than eight faulty nodes. For example, if u_{13} is fault-free, u_{12} is faulty, having passed u_{13}. Similarly, u_{11} is faulty, having passed u_{12}, etc. Indeed, if u_{13} is fault-free, there are at least seven other nodes that are faulty. There are seven definitely good units divided into two subsets $\{u_0, u_1, u_2, u_3\}$ and $\{u_{10}, u_{11}, u_{12}\}$ (indicated by the absence of shading). These are definitely good, since if any are faulty, we can identify more than eight faulty nodes. The remaining nodes are suspect (indicated by shading consisting of minuscule dots). These are divided into two subsets $\{u_6, u_7, u_8, u_9\}$ and $\{u_{15}, u_{16}, u_{17}, u_{18}\}$. The definitely bad and suspect nodes comprise the replacement set FR. Following the proof, let

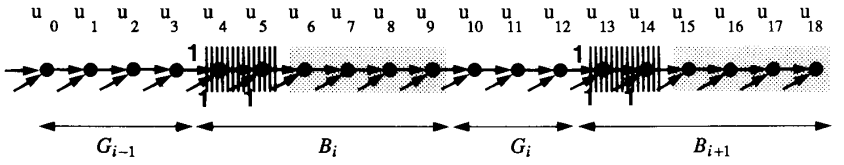
$$B_i = \{u_4, u_5, u_6, u_7, u_8, u_9\} \quad {}^*B_i = \{u_4, u_5\}$$

$$B_{i+1} = \{u_{13}, u_{14}, u_{15}, u_{16}, u_{17}, u_{18}\} \quad {}^*B_{i+1} = \{u_{13}, u_{14}\}.$$

$$G_i = \{u_{10}, u_{11}, u_{12}\} \quad G_i^{**} = \{u_{11}, u_{12}\}.$$

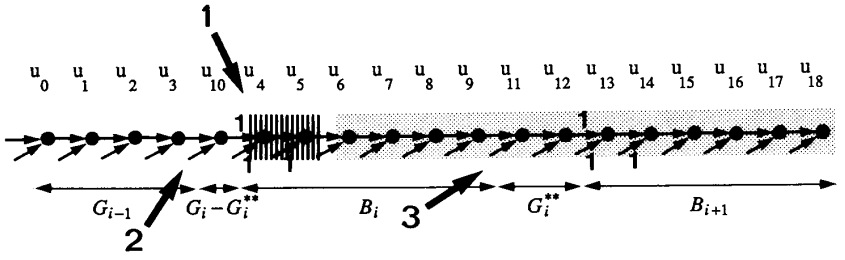
Thus, $FR = B_i \cup B_{i+1}$. ${}^*B_i$ and ${}^*B_{i+1}$ are the first $t = 2$ nodes in B_i and B_{i+1}, respectively. The proof of Lemma 1 shows that $|G_i| > |{}^*B_{i+1}|$. This is indeed true here.

Following the proof, we have $G_i - G_i^{**} = \{u_{10}\}$, which is removed and inserted immediately in front of ${}^*B_i$, that is, between u_3 and u_4. This yields the system of Fig. 6. The test results affected by the transplant of $G_i - G_i^{**} = \{u_{10}\}$ are outlined in Fig. 6. The numbers associated with arrows indicate the condition in the proof that specifies the test value. Considering the resulting syndrome, we find that the definitely bad, suspect, and definitely good nodes are as shown in Fig. 6. Specifically, u_4 and u_5 are definitely bad, as before. u_{13} and u_{14}, which were definitely bad, are now suspect. All suspect nodes before the change are still suspect. However, u_{11} and u_{12}, which were definitely good, are now suspect (for example, $\{u_4, u_5, u_6, u_7, u_8, u_9, u_{11}, u_{12}\}$ can be a set of faulty nodes which produces the syndrome shown). Thus, the total number of definitely bad and suspect nodes is larger by 2. This results in a contradiction; the claim that the original replacement set is maximal is wrong.



Definitely Bad Nodes - {[illegible]} and {[illegible]}
Suspect Nodes - $\{u_6, u_7, u_8, u_9\}$ and $\{u_{15}, u_{16}, u_{17}, u_{18}\}$
Definitely Good Nodes - $\{u_0, u_1, u_2, u_3\}$ and $\{u_{10}, u_{11}, u_{12}\}$

Fig. 5. Example of a $D_{1,2}(19)$ design with a replacement set that does not have consecutive nodes.



Definitely Bad Nodes - {[illegible]}
Suspect Nodes - $\{u_6, u_7, u_8, u_9, u_{11}, u_{12}, u_{13}, u_{14}, u_{15}, u_{16}, u_{17}, u_{18}\}$
Definitely Good Nodes - $\{u_0, u_1, u_2, u_3, u_{10}\}$

Fig. 6. The system of Fig. 5 rearranged to produce a larger replacement set.

Interestingly, the resulting replacement set consists of consecutive nodes. Indeed, it is a maximal replacement set.

ACKNOWLEDGMENT

The authors thank two referees for constructive comments.

REFERENCES

[1] K.-Y. Chwa and S. L. Hakimi, "On fault identification in diagnosable systems," *IEEE Trans. Comput.*, vol. C-30, pp. 414–422, June 1981.
[2] A. D. Friedman, "A new measure of digital system diagnosis," in *Dig. 1978 Int. Symp. Fault-Tolerant Comput.*, June 1975, pp. 167–170.
[3] S. L. Hakimi and A. T. Amin, "Characterization of the connection assignment problem of diagnosable systems," *IEEE Trans. Comput.*, vol. C-23, pp. 86–88, Jan. 1974.
[4] S. Karunanithi and A. D. Friedman, "Analysis of digital systems using a new measure of system diagnosis," *IEEE Trans. Comput.*, vol. C-28, pp. 121–133, Feb. 1979.
[5] A. Kavianpour and A. D. Friedman, "Efficient design of easily diagnosable systems," in *Proc. 3rd USA–Japan Comput. Conf.*, 1978, pp. 251–257.
[6] U. Manber, "Systems diagnosis with repair," *IEEE Trans. Comput.*, vol. C-29, pp. 934–937, Oct. 1980.
[7] F. Preparata, G. Metze, and R. Chien, "On the connection assignment problem of diagnosable system," *IEEE Trans. Electron. Comput.*, vol. EC-16, pp. 848–854, Dec. 1967.
[8] A. K. Somani, V. K. Agrawal, and D. Avis, "A generalized theory for system level diagnosis," *IEEE Trans. Comput.*, vol. C-36, pp. 538–546, May 1987.
[9] G. F. Sullivan, "A polynomial time algorithm for fault diagnosability," in *Proc. Foundations Comput. Sci.*, 1984, pp. 148–156.
[10] C.-L. Yang, G. M. Masson, and R. A. Leonetti, "On fault identification in t_1/t_1-diagnosable systems," *IEEE Trans. Comput.*, vol. C-35, pp. 639–643, July 1986.

Algorithm-Based Fault Detection for Signal Processing Applications

A. L. NARASIMHA REDDY AND P. BANERJEE

Abstract—**The increasing demands for high-performance signal processing along with the availability of inexpensive high-performance processors have resulted in numerous proposals for special-purpose array processors for signal processing applications. This correspondence presents a functional-level concurrent error-detection scheme for such VLSI signal processing architectures proposed for the FFT and *QR* factorization. Some basic properties involved in such computations are used to check the correctness of the computed output values. This fault detection scheme is shown to be applicable to a class of problems rather than a particular problem unlike the earlier algorithm-based error-detection techniques. The effects of roundoff/truncation errors due to finite-precision arithmetic are evaluated. It is shown that the error coverage is high with large word sizes.**

Index Terms—**Algorithm-based fault detection, FFT, finite-precision errors, *QR* factorization, signal processing applications.**

Manuscript received November 13, 1987; revised September 6, 1988. This work was supported in part by the National Science Foundation under Grant NSF MIP 86-19121 and in part by the Semiconductor Research Corporation under Contract SRC 87-DP-109.

The authors are with the Coordinated Science Laboratory and the Department of Electrical and Computer Engineering, University of Illinois, Urbana, IL 61801.

IEEE Log Number 9035137.